



9111-14 (non-Treasury)

**DEPARTMENT OF HOMELAND SECURITY**

Office of the Secretary

6 CFR Part 5

[Docket No. DHS 2013-0021

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** The Department of Homeland Security is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the “Department of Homeland Security/U.S. Customs and Border Protection – 019 Air and Marine Operations Surveillance System (AMOSS) System of Records” and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

**DATES:** Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit comments, identified by docket number DHS 2013-0021, by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.

- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office,  
Department of Homeland Security, Washington, D.C. 20528.

**INSTRUCTIONS:** All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

**DOCKET:** For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact: Laurence Castelli, (202) 325-0280, Privacy Officer, U.S. Customs and Border Protection, Washington, DC 20229. For privacy issues please contact: Jonathan R. Cantor (202-343-1717), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

**SUPPLEMENTARY INFORMATION:**

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) proposes to establish a new DHS system of records titled, “DHS/CBP - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records.”

The AMOSS System of Records Notice (SORN) is being published because AMOSS stores personally identifiable information in a system of records. AMOSS is a sophisticated radar processing system that supports the concerted and cooperative effort of air, land, and sea vehicles; field offices; and command and control centers staffed by

law enforcement officers (LEO), detection enforcement officers (DEO), pilots, crew, and Air and Marine Operations Center (AMOC) support staff in monitoring approaches to the U.S. border to detect illicit trafficking and direct interdiction actions, as appropriate. AMOSS also supports domestic operations in conjunction with other domestic law enforcement agencies by tracking domestic flights, as well as providing air traffic monitoring for air defense purposes. By processing a collection of external data imposed over a zooming-capable screen, AMOSS provides a real-time picture of air activity over a wide portion of North America, thus allowing system operators to discriminate between normal and suspicious air, ground, and marine vehicle movement. Much of the external data processed by AMOSS does not contain Personally Identifiable Information (PII) and is supplied to AMOSS by means of networked external sources. For instance, global positioning systems (GPS), maps, datasets from radar plot data, track data, and flight plan data are all incorporated to enhance the system operator's ability to discriminate between normal and suspicious aviation movement.

The collection of information in AMOSS is authorized primarily by the following authorities: 6 U.S.C. § 202; the Tariff Act of 1930, as amended, including 19 U.S.C. § 1590; 19 U.S.C. § 2075(b)(2)(B)(3); the Immigration and Nationality Act (INA), 8 U.S.C. § 1101, *et seq.*, including 8 U.S.C. §§ 1103, 1225, and 1324; and the Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. 104-208; Presidential Directive 47/Homeland Security Presidential Directive 16 (NSPD-47/HSPD-16); and DHS Delegation No. 7010.3 (May 11, 2006).

No exemption shall be asserted with respect to aircraft data collected from the FAA that is maintained in AMOSS. However, this FAA data may be shared with law

enforcement and/or intelligence agencies pursuant to the above routine uses. The Privacy Act requires DHS maintain an accounting of the disclosures made pursuant to all routine uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement or intelligence activity. As such, pursuant to 5 U.S.C. § 552a(j)(2), DHS will claim an exemption from (c)(3); (e)(8); and (g)(1) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from subsection (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(k)(2) as is necessary and appropriate to protect this information.

The Secretary of Homeland Security, pursuant to 5 U.S.C. § 552a(j)(2), has exempted all other AMOSS data from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. § 552a(k)(2), has exempted this non-FAA source data in AMOSS from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

## II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate personally identifiable information. The Privacy Act applies to

information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/U.S. Customs and Border Protection – 019 Air and Marine Operations Surveillance System (AMOSS) System of Records. Some information in DHS U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records relates to official DHS national security, law enforcement, immigration, and intelligence activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS's ability to obtain information from third parties and other

sources; and to protect the privacy of third parties. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis. Moreover, no exemption shall be asserted with respect to information maintained in the system as it relates to aircraft data collected from the FAA, aside from the accounting of disclosures with law enforcement and/or intelligence agencies pursuant to the routine uses in this SORN.

A notice of system of records for DHS U.S. Customs and Border Protection – 019 Air and Marine Operations Surveillance System (AMOSS) System of Records is also published in this issue of the Federal Register.

#### **List of Subjects in 6 CFR Part 5**

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

#### **PART 5--DISCLOSURE OF RECORDS AND INFORMATION**

1. The authority citation for Part 5 continues to read as follows:

**Authority:** 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. Add paragraph “72” at the end of Appendix C to Part 5 to read as follows:

#### **Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act**

\* \* \* \* \*

72. The DHS/U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security; and intelligence activities. The DHS/U.S. Customs and Border Protection - 019 Air and Marine Operations Surveillance System (AMOSS) System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

(a) No exemption shall be asserted with respect to aircraft data collected from the Federal Aviation Administration (FAA) that is maintained in AMOSS. However, this FAA data may be shared with law enforcement and/or intelligence agencies pursuant to the routine uses listed in the SORN. The Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routine uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement or intelligence activity. As such, pursuant to 5 U.S.C. § 552a(j)(2), DHS will claim an exemption from (c)(3); (e)(8); and (g)(1) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from subsection (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(k)(2) as is necessary and appropriate to protect this

information.

(b) The Secretary of Homeland Security, pursuant to exemption 5 U.S.C. 552a(j)(2) has exempted all other AMOSS data from the following provisions of the Privacy Act: 5 U.S.C. § 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); (f), and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this non-FAA source data in AMOSS from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

(c) When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

(d) Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (1) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or



evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(2) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(3) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(4) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would

alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

- (5) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.
- (6) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, potential witnesses, and confidential informants.
- (7) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.
- (8) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and

other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

- (9) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: August 6, 2013

Jonathan R. Cantor

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2013-22691 Filed 09/20/2013 at 8:45 am; Publication Date: 09/23/2013]